International Journal of Management (IJM)
Volume 11, Issue 8, August 2020, pp. 2216-2228, Article ID: IJM_11_08_192
Available online at http://www.iaeme.com/IJM/issues.asp?JType=IJM&VType=11&IType=8
Journal Impact Factor (2020): 10.1471 (Calculated by GISI) www.jifactor.com
ISSN Print: 0976-6502 and ISSN Online: 0976-6510
DOI: https://doi.org/10.34218/IJM.11.8.2020.192

RECOGNITION AND AVOIDANCE OF BLACKHOLE AND GRAYHOLE ATTACKS IN MANET USING NOVEL AUGMENTED AD HOC ON DEMAND DISTANCE VECTOR (AAODV)

Anu Sharma[1], Dr. Jitendra Sheetlani [2]

[1]Research Scholar, Department of Computer Science,
Sri Satya Sai University of Technology and Medical Sciences at Sehore, Madhya Pradesh, India

[2]Associate Professor, Department of Computer Science,
Sri Satya Sai University of Technology and Medical Sciences at Sehore, Madhya Pradesh, India

ABSTRACT

MANET network is a network consisting of a collection of nodes and its dynamic nature and can be made anywhere without using a fixed network infrastructure such as base station, making MANET vulnerable to attacks. One of several attacks that occur in the MANET network are black hole and gray hole attacks. Black hole attack is an attack that causes packets around the attacker's node to be lost so that network is at a loss and gray hole attack transmit the packets in inappropriate director or routes. Choosing the right routing protocol is one of the efforts to minimize the impact of black hole attacks. This research was made to enhance the behaviour of AODV routing protocols in minimize the impact of black hole and grey hole attacks. The results of this scheme indicate that proposed AAODV is better than AODV from several qualities of service values such as throughput, delay and packet loss

Key words: Security, Blackhole Attack, Grayhole Attack, AODV, MANET

Cite this Article: Anu Sharma and Jitendra Sheetlani, Recognition and Avoidance of Blackhole and Grayhole Attacks in Manet Using Novel Augmented Ad Hoc on Demand Distance Vector (AAODV), *International Journal of Management (IJM)*, 11(8), 2020, pp. 2216-2228.
http://www.iaeme.com/IJM/issues.asp?JType=IJM&VType=11&IType=8

1. INTRODUCTION

Today with new advances in the performance of communication technologies, advanced mobile wireless technology is expected to have an increasingly widespread application. MANET

mobile networks are networks that present solutions to wireless connections without the need to use a network infrastructure for their implementation; They dynamically create a network at any time and place, thus they provide mobility to the nodes so that the packets reach their destination, so it is necessary that all the nodes can fulfil the function of sender, receiver or routers; it also allows you to easily add and remove devices from the network [1].

Taking into account that the bandwidth is limited in a wireless channel, the nodes seek the assistance of neighbouring nodes for the forwarding of packets and therefore it can be affirmed that, in this type of networks, nodes can act as routers and hosts at the same time [2, 3].

These networks are very promising and popular in telecommunications, especially they are widely used in military applications, disaster areas and emergency operations such as search and rescue. The routing protocols [4] offered by this type of network are classified into Pro-active (DSDV, CGSR, OLSR, BATMAN, etc.), Reactive (AODV, DSR, TORA, etc.) and Hybrids (ZRP, SHARP, ZHLS, etc.), for this study the AODV and DSDV Protocols will be used.

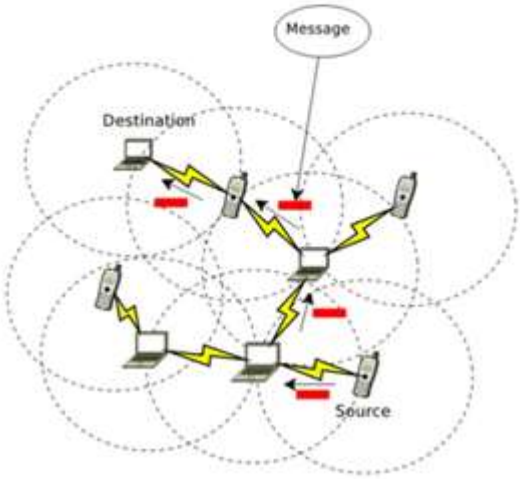


Figure 1 Mobile ad hoc networks

The Ad hoc On Demand Distance Vector (AODV) protocol is a reactive protocol that searches for a route only when a network node requires it, it is a protocol that needs little bandwidth because it sends packets only when necessary, although it causes high latency when connecting to the network. This IP routing protocol allows sending nodes to find and maintain routes to receiving nodes; here the protocol searches for possible routes only when there is a request and chooses the shortest route, that is, the one that responds first, keeping the routes active until they are not needed [7, 8].

The Destination Sequence Distance Vector (DSDV) protocol is based on the Bellman-Ford distribution algorithm (BDF) [5] which compared to the link state update method is computationally more efficient and requires much less storage space. In this algorithm, the neighboring nodes periodically exchange (proactive protocol) their complete routing tables with the neighbors to estimate the distance at which the other non-neighboring nodes are. Although DSDV only provides one path for each destination (it does not allow storing secondary or support routes), it always chooses the shortest path based on the number of hops to this destination.

The location of Nepal-Bihar near to Himalayas makes it very prone to the occurrence of natural disasters related to the movement of tectonic plates, catastrophes such as earthquakes show a high probability of occurrence, in addition to being very susceptible to the presence of strong monsoons, causing major flood emergencies especially in states like Chennai, Kerala,

Maharashtra and Bihar. One of the latest natural disasters, which has caused the most damage and losses in Nepal earthquake of 2015, also called Gorkha earthquake, severe earthquake that struck near the city of Kathmandu in central Nepal on April 25, 2015., this earthquake with a duration of 175 seconds and a magnitude of 7.8 on the Richter scale was one of the greatest tragedies the country has suffered which killed 8,964 people and injured 21,952 peoples [6].

In this event, communications failed, leaving a large part of the citizens without communication, and making it impossible for the arrival of rescue and relief aid. In the provinces affected by the disaster, access to mobile telephony and internet took days to be restored, since restoring a physical infrastructure is expensive and takes a long time, in these cases of disasters a MANET is an efficient option, since not requiring a fixed infrastructure is quick to implement and very useful to re-establish communications and carry out evacuation and rescue work in affected areas.

As Manet networks are a type of multi-hop wireless network made up of a group of devices called mobile nodes that are dynamically interconnected and related to each other to maintain network connectivity. They can be quickly deployed in unexpected conditions in response to disaster recovery, when it is difficult or impossible to immediately build a new fixed infrastructure, hence they are well suited to search operations, allowing rescue teams to take rapid action in response. to calls for help from victims.

In events such as the earthquake that occurred in the Province of Nepal and Bihar, thousands of people suffered due to the lack of coordination between relief organizations and one of the main reasons for this continues to be the destruction of communication channels in that area. Regarding the security of the area affected by the disaster, it is very important to process inquiries from outsiders to give a general picture of the evacuation process, injuries, emergency needs, etc.

In addition, to quickly manage and distribute food and vital supplies to evacuated residents, as well as to register and assign volunteers, the need for a reliable and high-bandwidth information and communication system is very important during this state of emergency. Wireless network properties, such as ease of deployment, freedom of connection, and communication via radio waves rather than data cables, ensure that wireless network technology is a perfect candidate for communication in areas of disaster.

However predict the situation where the MANET network itself is attacked by some malicious nodes like blackhole and grayhole attacks which lead to utter disaster in ad-hoc communication therefore this study depicts the scenarios how to eradicate the situation where the communication among the nodes is strong and affirm using the proposed scheme [9].

In this work one of the variables of the quality of service is examined, such as packet loss, end 2 end delay and throughput in Manet networks used by AODV and AAODV (proposed) routing protocols, analysing the advantages and disadvantages of the use of these protocols in disaster scenarios through a simulated environment, to determine which is the most appropriate and which allows stable and fast communication.

The following are the types of active attacks:

- Black hole: A black hole attack happens when a spiteful node which pretends having the shortest route to the target by sending the fake RREP to the source node and the drops the data blocks passing through it [10].
- Gray hole (Gray hole): By nature, Gray hole and Black hole attacks are almost similar. In Gray hole attack, the messages are dropped the same way they are dropped in black hole attack, but the difference is that this attack works in two treads. The first tread

involves the attacker node posing to have a legitimate route towards the destination and second tread wherein it starts to drop the captured packets when it gets the chance [11].

- Worm hole: This attack has also been named as Tunnel attack. In this attack, the malicious node shows a fictitious route pretending it to be the shorter than the original route. This creates a confusion in the network as the date packets are forwarded on the basis of distance between the two nodes. Here in this attack, that occurs one or more malicious nodes and a tunnel between them [12].
- Jellyfish attack: The nature of this attack varies from the above mentioned attacks. Here the malicious node, either delays their delivery or muddles their order or forwards them in an arbitrary manner rather than to drop them blindly [13].

2. LITERATURE STUDY

Researchers [14] have proposed a detection technique called SAODV to detect attacking node in the network. The technique works on the concept of neighbour opinion. According to this technique, every node in SAODV maintains two tables, to store ids of neighbour nodes and other for identification of route Reply received by every node against Route Request respectively. An opinion message is transmitted to neighbour nodes about the node advertising to have the record of activities performed by them. If the response of every node is NO, the particular node is detected as malicious node and a notification alarm is transmitted in the network. The major drawback of this approach is it incurs high overhead while sending opinion messages.

Researchers [15] in their research work have used simulation using 20, 50 and 100 nodes for detection of single and two malicious nodes and Intrusion Detection System to prevent the network from the attack of black hole nodes and enhance the network performance Packet Delivery Ratio, Throughput and reducing Packet Drop Rate using this technique. This technique could only work on Throughput only.

Researchers [16] have proposed a new algorithm named IDSAODV. They have simulated with AODV protocol with 20 nodes at a time and the same scenario is tested with the proposed mechanism. They again simulated 20 nodes using the proposed model and found that the effect of black hole node diminishes with the help of the proposed method. As per the researchers, packet loss got decreased by 66%.

Researchers [17] proposed a routing approach for detection and removal of malevolent node in the ad-hoc network. The technique is an EDRI based approach for detecting and removing attacker node and is based on the approach where a control data packet is used to check the nodes in the selected path with the help of an extended data routing table. As per the proposed technique, all the malicious nodes in selected path are selected and removed from the network. As the malicious nodes get removed from the network, this technique proves to be good as it decreases packet overhead and improves network throughput.

Researchers [18] have proposed GNBAODV: Guard Node Based-AODV to mitigate black hole attack in MANET. The proposed mechanism is based on special type of nodes which are helpful in detecting black hole nodes in the network. These guard nodes check the behaviour of the other nodes in the network and record the values of the same in a table. Each node has a trust value that is determined according to its behavior in the network, and it decreases when the node only sends RREP and does not send RREQ. If the trust value of a node decreases below the determined threshold, then it is blocked or isolated. Guard nodes broadcast an alarm to all adjacent nodes when a black-hole node is detected. The limitations of this system are that it needs a special type of nodes (guard nodes) and a huge number of guard nodes to cover all the network; also this system has a high overhead because of having many tables.

In [19] the state of the art in Blackhole and Grayhole attack detection solutions in MANET is studied and analyzed. In this work, a distinction is made between IDS solutions based on clustering, those based on cooperation between nodes, Multilayer, trust solutions, etc., the latter difficult to frame within a specific line of defense. The authors conclude the need for distributed solutions where nodes cooperate with each other, dynamic and lightweight among others, emphasizing the lack of solutions that include notification of the attack and its effective dissemination, as well as solutions focused on mitigating Blackhole attacks or Collaborative grayhole.

Researchers in [20] also devoted their efforts to classify and describe attacks on ad hoc networks, as well as a review of techniques that could be tolerant to threats. This paper focuses on Packet Dropping attacks, although it mentions many more. For the authors, the search for solutions that guarantee the continuity of the services supported by the network is decisive, and they make a very interesting reflection by proposing the investigation of solutions that act from all lines of defence as a single block.

Researchers in [21] present the benefits of the AODV protocol for MANET such as its dynamism. In turn, they review several works related to mitigating the Blackhole attack, which takes advantage of the weaknesses of this protocol. According to the authors, the most successful defenses come from methods based on some limit configured for some of the parameters related to the network, such as the Route REPly (RREP) or Route REQuest (RREQ) message count, once this limit is exceeded, the they will take the appropriate measures. This technique is known as the "tolerance" threshold.

3. RESEARCH METHODOLOGY

This section provides blueprint related to mobile ad hoc networks attacks namely black hole and grey hole. However, the AODV of routing protocols that exist for ad hoc networks dynamic routing. The main proposed operating aspects of the (augmented) AAODV protocol (proposed) is to provide the process of discovery of routes and maintenance of routes to provide the protection against the intrusion from Blackhole and Grayhole attacks and security-related issues. Consequently, the two main schemes of State-of-the-art will be proposed i.e. (Augmented) AAODV protocol as re-routing technique for the packets so it can be delivered to destination and to evaluate the QOS measures like end to end delay, throughput and packet loss along with intrusion detection as Blackhole and Gsrayhole.

3.1 General Description

3.1.1 AODV (Ad-Hoc On-Demand Distance Vector)

Ad-Hoc On-Demand Distance Vector, AODV, is a reactive protocol that has been adapted to work in mobile environments. This protocol maintains a route table to store routing information; stored routes are generated only when a node wants to send a packet. If the stored routes are requested within a period, they remain active; otherwise, they expire and a new one is searched when necessary.

3.1.2 AODV Routing Information

The intermediate nodes store all the information related to routing in route tables. Each node has as many entries in its table as destinations it knows. The fields that each record has are described below:

- *IP addresses*. Specify the source node and destination node IP addresses to find out where packets are coming from and going.

- *Sequence number*. The sequence number of the destination node allows to differentiate new information from obsolete information (the higher the number, the more up-to-date the route is; the older one can be discarded), in such a way that loops and old transmissions are prevented.
- *Target node sequence number validity indicator*. If when trying to communicate with a destination, negative results are obtained due to a link failure, or the route has in turn expired, the sequence number associated with that destination node is marked as invalid.
- *Other indicators on status and routes*. There are indicators on whether or not the route is valid, and in the latter case if it is repairable, it is not repairable and an alternative path must be sought.
- *Network interface*. The AODV operation must be correct for both wired and wireless networks; from there arises the importance that this protocol knows the interface through which the packets arrive. This includes receiving RREQ, RREP, and RERR messages. Similarly, each time you learn a route to a new destination, the interface through which the destination can be reached is also recorded in the destination route table entry.
- *Number of hops (hop count)*. It tells the source node the number of hops required to reach a destination node.
- *Next jump*. Adjacent node through which packets travel until reaching the desired destination.
- *List of precursors*. Set of nodes that make up the path resulting from the path discovery process.
- *Route life time (lifetime)*. Routes have a duration time after which they must be removed to prevent lost messages from flooding the network.

3.1.3 AODV Message Formats

AODV for its operation makes use of the following types of messages:

- Route Request (RREQ)
- Route Reply (RREP)
- Route Error (RERR)
- Route Reply-Acknowledge (RREP-ACK).
- The formats that AODV messages have are detailed below.
- Route Request (RREQ)

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |J|R|G|D|U|   Reserved          | Hop Count     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                            RREQ ID                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Destination IP Address                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Destination Sequence Number                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Originator IP Address                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Originator Sequence Number                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 2 Details of the Message Format Route Request (RREQ)

4. RESEARCH FLOWCHART

The following is a flow chart of the research that will be carried out related to the optimization of protocol performance routing AAODV (proposed) using the RREQ method to protect the nodes from black hole and grey hole attacks as in Figure 3.

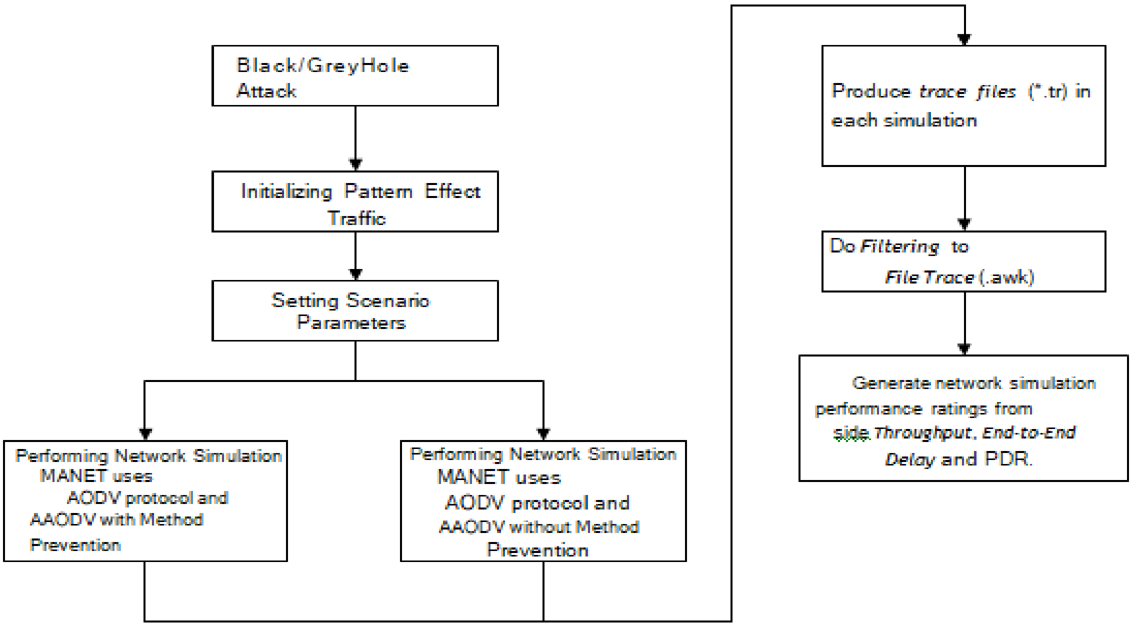


Figure 3 Detailed Explanation

5. METHODOLOGY

MANET network using the protocol routing AODV and AAODV. In this simulation, the researcher applies the attack Route Request (RREQ) for Black Hole and Grey Hole Attacks. In this case the RREQ Black Hole and Grey Hole attacks apply the concept of a packet drop or abnormal behavior attack by generating nodes fake to overwhelm nodes original with broadcast False RREQ to interrupt the process of determining the route of data transmission.

Authors of this research through research methodology have explained as to how to find the existence of attacker node and set it apart from the network by utilizing information carried by a packet containing information about the presence of a malicious node which has been detected. This study also discusses the aftermaths of black hole and grey hole attack on parameters like Throughput, E2E delay and PDR.

5.1 Scenario Design

The scheme begins with designing test scenarios for sending packages from origin node to goal node with existence of black holes in MANET. In this simulation, there are several nodes with designated roles:

Source node: This is the starting node for packet delivery.

Intermediate nodes: It is the packet distribution node from origin node to goal node.

Destination node: This is final node for receiving data blocks from origin node or node to which origin node forwards data blocks.

Black hole node: The node which acts maliciously and packets sent through this never reach the destination node.

Grey hole node: The node which acts abnormally and packets sent through this never reach the destination node.

5.2. AAODV Method Design

In this section, the researcher conducts the process of designing a method to take preventive measures against RREQ attacks flooding, namely AAOD. Where is this AAODV scheme done by finding nodes indicated as malicious nodes and will be restored to nodes normal. By taking AAODV countermeasures, can reduce the impact of RREQ black hole and grey hole attacks flooding, i.e. the reduced action of sending fake RREQs by black hole and grey hole through the isolation process from the network within a certain period of time, thereby reducing the burden bandwidth network which causes the quality of data transmission to increase.

5.3 Network Simulation Scenario Design

The following is a flow diagram of the MANET network simulation scenario planning process related to research in optimizing network security quality on the AODV and AAODV protocols with the black hole and grey hole prevention method due to RREQ attacks.

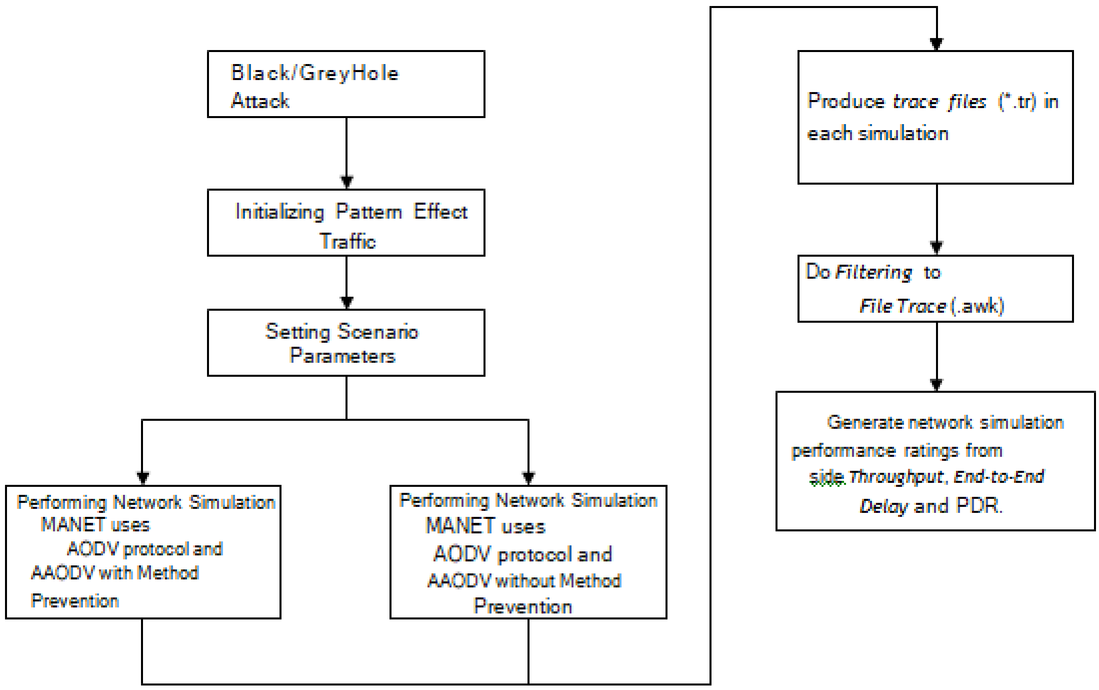


Figure 4 Simulation Scenario Block Diagram

6. PROPOSED ALGORITHM (AAODV) – AUGUMENTED AD HOC ON-DEMAND DISTANCE VECTOR:

Input: Routing Table with Reply Packets, t- time in which the RREQ was received, RRQT - Request Sent Table

Output: Detection of Destination Node, Transmission Node, Black Hole Node and Grey Hole Node with Routing Table updated State flags.

Beginning

1: Add Total Number of Nodes and Routing Time “t” to RRQT- Table of Replies received

2: If (RRQT == RREQ) then

3: Status = Free

4: VERIFY Destination Node (RREQ, t)

5: Fate EVALUATE E2D DELAY, PACKET LOSS AND THROUGHPUT

6: If ((RREQ == Node (Black Hole) && RREP == Node (Grey Hole)) &&
(RRQT != RREP[t])) (for some t, 1≤ t ≤ MAXTIME)) then

7: EXIT RERR (ROUTE ERROR)

8: Fate MALICIOUS NODE EXISTS THEREFORE EVALUATE/CALCULATE E2D DELAY, PACKET LOSS AND THROUGHPUT

9: If (RERR != RREQ [i] (for some i, 1 ≤ i ≤ RQTMAX)) then

10: If (RREQ == RREP-ACK [j] (for some j, 1≤ j ≤ NEXT_HOP_WAIT))
then

11: If (RREQ <= PATH DISCOVERY TIME [j]) then NEXT_HOP = NEXT_HOP + 1

12: Status = TTL START

13: Fate NEW INTERMEDIATE NODE FOUND

14: Status = TTL INCREMENT

15: End_Yes

16: Fate PACKET DELIVERED THEREFORE EVALUATE/CALCULATE E2D DELAY, PACKET LOSS AND THROUGHPUT

17: VERIFY DESTINATION NODE (RREP, t) (Packet Deliver Successfully to Destination)

18: End_Yes

19: Fate

20: Status = RERR - "Possible black or Grey Hole Attack"

21: End_Yes

22: End_Yes

23: End_Yes

The end

7. SIMULATION AND RESULTS

Although MANET has independent nodes, as well as flexible and dynamic routing, the securities in MANET are completely different from securities in conventional networks. Therefore, network security problems in MANET are a serious problem. Like a network in general, MANET is not immune from external attacks nodes that do not run according to their duties are called malicious nodes, among them is a black hole and grey hole. Black hole attacks cause packets that should be sent to the destination are not sent, nodes attacked by black holes will become malicious nodes which, if passed, will discard packets sent to that node instead of sending them to other nodes to be delivered to the destination node whereas the grey hole node acts abnormally and start sending the messages to different intermediate nodes which is not in the path for the destination. In addition, the malicious node will promote itself as the best path for packets to reach their destination, so that packets will more easily enter through nodes affected by black-hole and grey-hole attacks.

The routing protocol in MANET has a different way of routing and choosing different paths. The resulting performance and quality of services have different values. By testing different routing protocols, the performance comparison of the two routing protocols can be known, and it can be sorted out which one is better in dealing with black hole attacks. The topic of this study

is to analyze the performance of MANET using the AODV and proposed AAODV routing protocol with rushing and black hole and grey hole attacks based on the parameters of packet delivery ratio, throughput, and end-to-end delay.

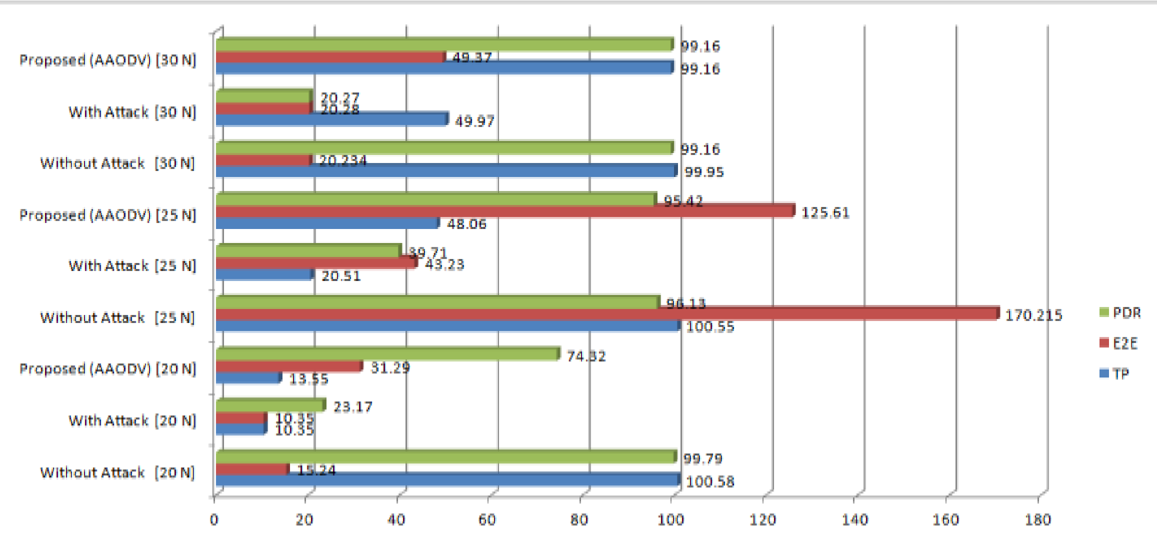
7.1 Parameters for Testing

The design of the test scenario is carried out to see and measure the accomplishment of the protocol against scenario of attacker node position, movement type and the number of nodes. From the test scenario data will be obtained to analyze the protocol. The design can be seen as under:-

Table 1 Configuration of black/grey hole position variations

S.NO	PARAMETER	INFORMATION
1	ROUTING PROTOCOL	AODV/AAODV
2	NOS. OF NODES	20,25 AND 30
3	NOS. BLACK/GREY HOLE NODES	2 TO 4
4	CONNECTION TYPE	UDP
5	TYPE OF PACKETS	CBR
6	SIZE OF PACKETS	1024 BYTES
7	PACKETS CBR RATE	KBPS
8	AREA	600 METERS * 600 METERS
9	SIMULATION TIME	1000 SECONDS
10	MOBILITY TYPE	CONSTANT
11	NODE SPEED	1 TO 100 M/S

In accordance with the formulation of the problem that the author made, after all parameters are obtained, then the next step is to compare the results of the scenarios that have been executed. Then in the level analysis vulnerabilities of greyhole attacks and blackhole attacks on the protocol AODV and AAODV for 20, 25 and 30 Nodes are as under



	Without Attack [20 N]	With Attack [20 N]	Proposed (AAODV) [20 N]	Without Attack [25 N]	With Attack [25 N]	Proposed (AAODV) [25 N]	Without Attack [30 N]	With Attack [30 N]	Proposed (AAODV) [30 N]
PDR	99.79	23.17	74.32	96.13	39.71	95.42	99.16	20.27	99.16
E2E	15.24	10.35	31.29	170.215	43.23	125.61	20.234	20.28	49.37
TP	100.58	10.35	13.55	100.55	20.51	48.06	99.95	49.97	99.16

Figure 5 Collective Results of All Scenarios without attack, with attacks and with using AODV and proposed AAODV Algorithm

Figure 6 above shows a comparison of the value of the packet delivery ratio, throughput and end 2 end delay of the AODV and AAODV (proposed) routing protocol on the black hole and grey hole attacks patterns on the 20, 25 and 30 node variant respectively. It can be seen that the PDR value is very less when the black hole attack and the majority of packet loss is there. However, due to black and grey hole attacks there are packets that are wasted and do not arrive at their destination. Likewise in figure 4.21 above shows a comparison of the value of the throughput is declined where the black hole or grey hole occurs utilizing the AODV routing protocol on the pattern of the 20, 25 and 30 node variant. It can be seen that the black/grey hole attack has a lesser throughput values. Subsequently, the end 2 end delay is also very less while transmitting the packets.

Based on the problem formulation and explanation that the researchers described in the first chapter, the researchers can draw conclusions, namely: The percentage of data packets received or wasted when exposed to blackhole and grey hole attacks on the MANET network with 20, 25 and 30 nodes, The AODV routing protocol has a vulnerability to black and grey hole attacks. With the comparison results in the form of two attack patterns, the AAODV proposed) is the effective technique/model or algorithm to protect the packets from the black hole and grey hole and to retransmit the data packets to destination amicably

8. CONCLUSION

From the research that has been done, several conclusions can be drawn:

- In the throughput test parameter, AAODV (proposed) has better performance compared to AODV. Especially when the MANET network is hit by a black and grey hole attacks. AODV protocol decreased by 13.55% in 20 nodes, 20.51% in 25 nodes and 49.97%, in 30 nodes whereas the proposed AAODV is successfully able to recover 13.55% in 20 nodes, 48.06% with 25 nodes and 99.16% in 30 nodes respectively.
- Thereinafter, the E2E delay test parameter, AAODV (proposed) also achieved the better performance compared to AODV. Likewise, when the MANET network is hit by a black and grey hole attacks. AODV protocol decreased by 10.35ms in 20 nodes, 43.23ms in 25 nodes and 20.27ms, in 30 nodes whereas the using the proposed AAODV is successfully able to recover 31.29ms in 20 nodes, 125.61ms with 25 nodes and 49.37ms in 30 nodes respectively. Consequently, the packet was delivered successfully therefore, the 2E2 delay is higher.
- Last but not least, the essential and crucial PDR test parameter, AAODV (proposed) amicably achieved the optimal performance compared to AODV. However, when the MANET network is hit by a black and grey hole attacks. AODV protocol decreased by 23.17% in 20 nodes, 39.71% in 25 nodes and 20.27% in 30 nodes lastly, using the proposed AAODV is successfully able to recover 74.32.% in 20 nodes, 95.42% with 25 nodes and 99.16% in 30 nodes respectively.

As per the above parameters, AAODV is also better than AODV. This is indicated by the values of percent of AAODV which experienced a considerable increase compared to AODV when hit by collaborative black hole and grey hole attacks. Thus AAODV routing protocol is better than AODV protocol from several aspects of research especially on networks affected by black holes and grey holes. The two of them experienced some performance decline, but AAODV showed an acceptable elevation. Therefore, as per the proposed scheme under the black hole and grey hole attacks it is recommended to transmit the packets using the proposed AAODV technique for better availability, maintainability and reliability of data.

REFERENCES

[1] Alomari, Saleh & Putra, Sumari. (2010). An Overview of Mobile Ad Hoc Networks for the Existing Protocols and Applications. CoRR. abs/1003.3565. 10.5121/jgraphhoc.2010.2107.

[2] Lalar, Sachin & Yadav, Arun. (2017). Comparative Study of Routing Protocols in MANET. Oriental journal of computer science and technology. 10. 174-179. 10.13005/ojcst/10.01.23.

[3] Fihri, Mohammed & Badr, Chahidi & Ezzati, Abdellah. (2014). Comparative study of routing protocols in MANET. International Conference on Next Generation Networks and Services, NGNS. 149-153. 10.1109/NGNS.2014.6990244.

[4] Natarajan, Kannan & Sethuraman, Priya. (2017). Refined trust energy-ad hoc on demand distance vector (ReTE-AODV) routing algorithm for secured routing in MANET. Wireless Networks. 23. 2227-2237. 10.1007/s11276-016-1284-1.

[5] He, Guoyou. (2002). Destination-Sequenced Distance Vector (DSDV) Protocol.

[6] https://en.wikipedia.org/wiki/April_2015_Nepal_earthquake

[7] Perkins, Charles & Belding, Elizabeth. (1999). Ad-hoc On-Demand Distance Vector Routing. Proc. 2nd IEEE Workshop on Mobile Computing Syst. and Applications (WMCSA '99) (New Orleans, LA. 25. 90-100. 10.1109/MCSA.1999.749281.

[8] Pal, Purba & Sarkar, Priya & Deb, Sonali & Bhattacharya, Gourab. (2019). Analysis of AODV Protocol in MANET. International Journal of Computer Applications. 177. 1-6. 10.5120/ijca2019919691.

[9] Chaitanya, K. & Venkateswarlu, S.. (2016). Detection of Blackhole & greyhole attacks in MANETs based on acknowledgement based approach. 89. 210-217.

[10] Oakley, Ian. (2020). Solutions to Black Hole Attacks in MANETs. 1-6. 10.1109/CSNDSP49049.2020.9249524.

[11] Patil, Sarika. (2017). Gray hole attack detection in MANETs. 20-26. 10.1109/I2CT.2017.8226087.

[12] Babu, A. & Nagendranath, M.V.S.S.. (2017). Adverse effect of black hole and worm hole attacks on MANETs. International Journal of Applied Engineering Research. 12. 9245-9252.

[13] Kaur, Simranpreet & Kaur, Rupinderdeep & Verma, A.K.. (2015). Jellyfish attack in MANETs: A review. 1-5. 10.1109/ICECCT.2015.7226168.

[14] Dhende, Sandeep & Musale, Sandeep & Shirbahadurkar, Suresh & Najan, Anand. (2017). SAODV: Black hole and gray hole attack detection protocol in MANETs. 2391-2394. 10.1109/WiSPNET.2017.8300188.

[15] K. Madhuri, N. K. Viswanath and P. U. Gayatri, "Performance evaluation of AODV under Black hole attack in MANET using NS2," 2016 International Conference on ICT in Business Industry & Government (ICTBIG), 2016, pp. 1-3, doi: 10.1109/ICTBIG.2016.7892661.

[16] SiddharthDhama, Sandeep Sharma, MukulSaini, "Black Hole Attack Detection and Prevention Mechanism for Mobile Ad-Hoc Networks" Published in: Computing for Sustainable Global Development (INDIACom), 2016 3rd International Conference on Date of Conference: 16-18 March 2016.

[17] Dorri, Ali. (2017). An EDRI-based approach for detecting and eliminating cooperative black hole nodes in MANET. Wireless Networks. 23. 10.1007/s11276-016-1251-x.

[18] Rajeswari, A., Kulothungan, K., & Kannan, A. (2016). GNB-AODV : Guard Node Based – AODV to Mitigate Black Hole Attack in MANET. International journal of scientific research in science, engineering and technology, 2, 671-677.

[19] Ali Zardari, Zulfiqar & He, Jingsha & Zhu, Nafei & Hussain, Khalid & Pathan, Muhammad Salman & Hussain, Muhammad Iftikhar & Memon, Muhammad Qasim. (2019). A Dual Attack Detection Technique to Identify Black and Gray Hole Attacks Using an Intrusion Detection System and a Connected Dominating Set in MANETs. Future Internet. 11. 61. 10.3390/fi11030061.

[20] Sánchez-Casado, Leovigildo & Magán-Carrión, Roberto & García-Teodoro, Pedro & Díaz-Verdejo, Jesús. (2014). Defenses against Packet-Dropping Attacks in Wireless Multihop Ad Hoc Networks. Security for Multihop Wireless Networks. 377-400. 10.1201/b16754-18.

[21] Nital Mistry, Devesh C Jinwala, Mukesh Zaveri,"Improving AODV Protocol against Blackhole Attacks," Procedings of the international multi conference of engineer and computer science Vol 2, 2010.